

CLAIMS

1 1. Method for verifying the usage of public keys derived from a set of
2 asymmetric keys, a public key (K_p) and private key (K_s) generated for a given use, such as
3 encryption/decryption or digital signature verification/generation, by an embedded system
4 and stored in the storage area of an embedded system (S_i) equipped with cryptographic
5 calculation means and externally accessible read/write-protected means for storing digital
6 data, this digital data (ID_{d_i}) comprising at least a serial number (SN_i) for identifying the
7 embedded system and an identification code (Op_j) of an operator authorized to configure said
8 embedded system, this request being formulated by said embedded system by transmitting a
9 request message (MRCA) containing said public key (K_p) to a certification authority (CA),
10 characterized in that this process consists:

11 - prior to any transmission of a certification request, during the configuration of these
12 embedded systems by this authorized operator for all the embedded systems (S_i) of a set (L_k)
13 of embedded systems:

14 - of having this authorized operator generate, for this set of embedded systems, a

15 mother public key (K_{pM}) and a mother private key (K_{sM}) used in connection with a process
16 supported by an algorithm (CA1M);

17 - of publishing said mother private key (K_{pM}) associated with the algorithm (CA1M),
18 the identity of this authorized operator (OP_j), and with a set (L_k) defining a range of
19 embedded system identifiers;

20 - of calculating, for each embedded system belonging to this set (L_k) of embedded
21 systems, from said mother private key (K_{sM}) and from the serial number (SN_i) of the
22 embedded system, a diversified private key (K_{sMi}), and of storing said diversified private key
23 (K_{sMi}) in said externally accessible, read/write-protected storage area, and;

24 - prior to any transmission of a certification request message:

25 - of having the embedded system generate a certification request (RCA) containing, in
26 particular, a field of the public key (CA1, K_p) and the usage indicators (U) of this public key,

27 - of calculating, using said calculation means and said diversified key (K_{sMi})

28 associated with this embedded system, a cryptographic control value (S_{ci}) on the entire
29 request (RCA), said cryptographic control value being a digital signature calculated by means
30 of the diversified private key (K_{sMi});

31 when a certification request is sent to the certification authority by the embedded
32 system:
33 - of forming a certification request message (MRCA) containing the request (RCA), the
34 identifier (IDd_i) of the embedded system, the latter being constituted by the identifier (OP_j) of
35 this authorized operator and by the serial number (SN_i) of the embedded system, and the
36 cryptographic control value (Sc_i);
37 - of transmitting to the certification authority (CA) said request message (MRCA)
38 formed during the preceding phase and containing the public key (Kp) and the usage
39 indicators (U) subject to said certification, and said cryptographic control value (Sc_i);
40 · when a certification request message (MRCA) is received by the certification
41 authority:
42 - of retrieving the identity of the authorized operator (OP_j) from the identifier (IDd_i) of
43 the embedded system,
44 - of retrieving, from said identifier (OP_j) of this authorized operator, the value of the
45 mother public key (KpM) as well as the identifier of the algorithm (CA1M) associated with
46 the set to which the embedded system belongs,
47 - of verifying, from said mother public key (KpM), from said serial number (SN_i) of the
48 embedded system, and from said certification request message (MRCA) received, said
49 cryptographic control value (Sc_i), which makes it possible to establish the authenticity of this
50 cryptographic control value and the source of this certification request.

1 2. Method according to claim 1, characterized in that when the certification
2 request is generated by the embedded system, the method also consists of generating, at the
3 embedded system level, the certification request (RCA), which is composed of three fields,
4 i.e.: a public key algorithm identifier (CA1), a public key value (Kp), and an indicator of the
5 usages of this key (U).

1 3. Method according to claim 1, characterized in that when the certification
2 request is completed by the embedded system during the step consisting of communicating a
3 certification request template (GRCA) to said embedded system, the method also consists:
4 - of checking, at the embedded system level, the syntax of the certification request
5 template (GRCA) in order to make sure that it is a correctly formed certification request, and

6 - of conditioning the step consisting of having the embedded system fill in the missing
7 fields of the certification request template (GRCA) to a positive verification.

1 4. Method according to claim 1, characterized in that, for a set of asymmetric
2 signature keys (Kp), (Ks) generated by said embedded system, the cryptographic calculation
3 means of this embedded system allowing the use of the private key (Ks) only for signature
4 generation purposes, said private key (Ks) stored in said externally accessible read/write-
5 protected storage area being unknown to the user and limited to a utilization exclusively for
6 digital signature purposes, the utilization of said key is limited to signature purposes and the
7 utilization of the certificate containing the corresponding public key is limited, in practice, to
8 signature verification purposes.

1 5. Method according to claim 1, characterized in that for a set of asymmetric
2 keys, a public encryption key (Ep) and a private decryption key (Ds) generated by said
3 embedded system, the method consists of associating, with said keys (Ep), (Ds) and with the
4 asymmetric decryption process, a symmetric "weak" decryption process and key, the
5 symmetric decryption key being encrypted, then decrypted, by means of the private
6 asymmetric decryption key (Ds), said private key (Ds) stored in said externally accessible
7 read/write protected storage area being unknown to the user, which makes it possible to
8 authorize the utilization of said key only for weak decryption purposes, the utilization of the
9 certificate containing the corresponding public key being limited, in practice, to weak
10 encryption purposes.

1 6. Embedded system comprising a calculation unit, a RAM, a nonvolatile
2 memory comprising a programmable memory comprising an externally accessible protected
3 storage area, a cryptographic calculation module and an input/output system connected by a
4 link of the BUS type, characterized in that said embedded system comprises at least:
5 - a diversified key KsM_i stored in said externally accessible protected memory, said
6 diversified private key, unique and distinct for this embedded system and calculated from a
7 mother private key KsM and an identification number of this embedded system, being
8 associated with a mother public key KpM; said cryptographic calculation module comprising:
9 - means for calculating a signature from said diversified private key KsM_i, making it
10 possible to calculate the signature of a request to certify a public key Kp associated with a

11 private encryption key K_s or signature key, respectively, said private key K_s generated by
12 said signature calculation means being stored in said protected memory, this signature of a
13 certification request being a function of the identification number of this embedded system,
14 said signature calculation means making it possible to transmit to a certification authority a
15 certification request message containing said certification request and said signature, which
16 allows said certification authority to verify the source of the certification request from this
17 embedded system and the protection of said diversified private key and private signature key
18 in said externally accessible protected memory using only public elements, such as said
19 mother public key K_{pM}.

*Add
A4*